Cyber Grand Challenge

Rules
May 16, 2014

Version 2

Defense Advanced Research Projects Agency
Information Innovation Office
675 North Randolph Street
Arlington, VA 22203-2114

CYBER

GRAND_CHALLENGE

Document Change Summary

Section	Description	Date
2.3	Open Track Application Deadline Extended	14 May 2014

Table of Contents

1 Introduction 5

1.1 Vision 5

1.2 Overview 5

1.3 Objectives 6

2 Applying to the Cyber Grand Challenge (CGC) 7

2.1 Eligibility 7

2.2 Proposal Track Applications 8

2.3 Open Track Applications 8

3 Cyber Grand Challenge Events 9

3.1 Cyber Grand Challenge Qualification Event (CQE) 9

3.1.1 Preparing for CQE 9

3.1.2 CQE Scoring 9

3.1.3 Advancement to CFE 10

3.1.4 Finalists 10

3.2 Cyber Grand Challenge Final Event (CFE) 11

3.2.1 CFE Trials 11

3.2.2 CFE Format 12

3.2.3 CFE Scoring 12

3.2.4 CFE Technical Paper 13

3.2.5 CFE Prizes 13

4 Full Automation Requirement 13

5 Intellectual Property 14

6 Additional Information 14

7 Scope and Precedence 16

1 Introduction

1.1 Vision

Top computer security experts test their skill head-to-head in competitive "Capture the Flag" contests. These contests provide a competition rating for the ability of experts to locate and comprehend security weaknesses.

The Defense Advanced Research Projects Agency (DARPA) Cyber Grand Challenge (CGC) will utilize a series of competition events to test the abilities of a new generation of fully automated cyber defense systems. During a final competition event, automated Cyber Reasoning Systems will compete against each other in real time. This event will be held in a public setting and documented for research purposes.

The CGC seeks to engender a new generation of autonomous cyber defense capabilities that combine the speed and scale of automation with reasoning abilities exceeding those of human experts.

1.2 Overview

The Department of Defense (DoD) maintains information systems using a software technology base comprised of Commercial Off The Shelf (COTS) operating systems and applications. This COTS technology base is common to the DoD, industry, and the Defense Industrial Base, and the continual discovery of potential vulnerabilities in this software base has led to a constant cycle of intrusion, compromise discovery, patch formulation, patch deployment and recovery. This defensive cycle is currently performed by highly trained software analysts; it is the role of these analysts to reason about the function of software, identify novel threats and remove them. Manual analysis of code and threats is an artisan process, often requiring skilled analysts to spend weeks or months analyzing a problem. The size of the technology base also contributes to the difficulty of manually discovering vulnerabilities.

At the present time, automated program analysis capabilities are able to assist the work of human software analysts. These automation technologies include Dynamic Analysis, Static Analysis, Symbolic Execution, Constraint Solving, Data Flow Tracking, Fuzz Testing, and a multitude of related technologies. In the Cyber Grand Challenge, a competitor will improve and combine these semi-automated technologies into an unmanned Cyber Reasoning System (CRS) that can autonomously reason about novel program flaws, prove the existence of flaws in networked applications, and formulate effective defenses. The performance of these automated systems will be evaluated through head-to-head tournament style competition.

The CGC program will draw widespread attention to the technology issues associated with autonomous software comprehension and motivate entrants to overcome technical challenges to realize truly effective autonomous cyber defense. This program

will challenge the most capable and innovative companies, institutions, and entrepreneurs to produce breakthroughs in capability and performance.

1.3 Objectives

Currently, network Intrusion Detection Systems, software security patches, and vulnerability scanners are all forms of *signature based defense:* defensive systems which act on discrete quanta of human knowledge ("signatures"). Human analysts develop these signatures through a process of reasoning about software. In fully autonomous defense, a cyber system capable of reasoning about software will create its own knowledge, autonomously emitting and using knowledge quanta such as vulnerability scanner signatures, intrusion detection signatures, and security patches.

The objective of this program is to identify effective, integrated automation of cyber reasoning tasks as assessed by the Areas of Excellence (AoE) in Table 1. These AoE address the protection of compiled test software ("Challenge Binaries" or "CBs") operated on a closed, monitored network ("Competition Framework").

	Areas of Excellence (AoE)	**CGC Qualification Event (CQE)**	**CGC Final Event (CFE)**
1	**Autonomous Analysis**: The automated comprehension of computer software (e.g., CBs) provided through a Competition Framework.	✓	✓
2	**Autonomous Patching:** The automatic patching of security flaws in CBs provided through a Competition Framework.	✓	✓
3	**Autonomous Vulnerability Scanning:** The ability to construct input which when transmitted over a network provides proof of the existence of flaws in CBs operated by competitors. These inputs shall be regarded as Proofs of Vulnerability.	✓	✓
4	**Autonomous Service Resiliency:** The ability to maintain the availability and intended function of CBs provided through a Competition Framework.	✓	✓
5	**Autonomous Network Defense:** The ability to discover and mitigate security flaws in CBs from the vantage point of a network security device.		✓

Table 1 - Areas of Excellence

2 Applying to the Cyber Grand Challenge (CGC)

DARPA provides two parallel paths for participating in the CGC: the Proposal Track and the Open Track. Rankings in the CGC Qualifying Event (CQE) and the CGC Final Event (CFE) will be based on the same technical evaluation criteria and scoring mechanisms for all competitors, irrespective of track. Proposal Track and Open Track teams that successfully pass the CQE will be invited to compete in the CFE. See Section 3 for a detailed description of the CQE and CFE.

2.1 Eligibility[1]

A CGC Team is comprised of an entrant (US Entity[2] or individual), an individual team leader and an optional set of team members (individuals). Individual entrants may be the same individual named as team leader. If the entrant is a US Entity rather than an individual, the team must identify an entrant official. Teams may enter under an official affiliation (e.g., a university or corporation). Teams may also have an official set of sponsors.

Cyber Grand Challenge Team

Entrant	Team Leader	Team Member(s)	Sponsor(s)	Official Affiliation
Required	Required	Optional	Optional	Optional
US Entity or individual(s)	Individual	Individual(s)	US Entity or individual(s)	US Entity

The CGC is open to team members of all nationalities and of all ages with the following caveats:

- CGC participation by minors requires authorization by a parent or guardian.
- An entrant must be a U.S. citizen, permanent resident, or US Entity.
- An individual, organization, or sponsor is not eligible to apply or participate if he, she, or it is on the Specially Designated Nationals list.[3]

Teams are intended to be wholly separate entities that do not share members, unique technology, official affiliations or financial interest.

[1] This section specifically refers to eligibility to participate in CGC events; eligibility to receive prizes is based on 15 U.S.C. § 3719. See DARPA-BAA-14-03 and DARPA-BAA-14-05 for specifics regarding eligibility to propose to those solicitations.

[2] Within these Rules, a US Entity is defined as a private entity incorporated in and maintaining a primary place of business within the United States; see 15 U.S.C. § 3719(g)(3).

[3] http://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx.

Federal entities (from the US or any other country) are not eligible to participate as entrants, sponsors or official affiliates. Federal employees acting within the scope of their employment are not eligible to participate as entrants, entrant officials, team leaders or team members.

A Federal employee acting outside the scope of his or her employment should consult his or her ethics official before participating in the Challenge. DARPA employees and support contractors, their spouses, dependents, and household members are not eligible to participate.

Any personnel funded by DARPA to support the Cyber Grand Challenge are not eligible to participate. This group includes, but is not limited to, any party funded under DARPA-BAA-14-03 as well as any Federally Funded Research and Development Center (FFRDC) or Government personnel whose scope of work covers CGC architecture development.

DARPA reserves the right to disqualify a participant whose actions are deemed to violate the spirit of the competition for any reason, including but not limited to, the violation of relevant laws or regulations in the course of participation in the Challenge.

See Section 6 for additional information.

2.2 Proposal Track Applications

Proposal Track teams will be competitively selected on the basis of proposals submitted in response to DARPA-BAA-14-05. See DARPA-BAA-14-05 for Proposal Track deadlines and procedures related to submissions and selections. Proposal Track teams receiving an award through Broad Agency Announcement (BAA) DARPA-BAA-14-05 may not participate in the Open Track.

2.3 Open Track Applications

There is no fee for entry. Application materials are available on the Cyber Grand Challenge website (www.darpa.mil/cybergrandchallenge) and must be submitted in accordance with the instructions outlined herein. The application procedure is a two-step process consisting of an initial application and an extended application. All parts of both applications must be received by DARPA no later than 12:00 noon (U.S. Eastern Time), ~~June 3, 2014~~ November 2, 2014.

DARPA will acknowledge receipt of complete applications via e-mail. Upon receipt of each team's Cyber Grand Challenge Initial Application, DARPA will assign a team reference number which should be included on all team correspondence with DARPA.

The Initial Application must be submitted online at:
www.darpa.mil/cybergrandchallenge.

The Extended Application may be submitted through one of the detailed methods below.

(1) E-mailed to CyberGrandChallenge@darpa.mil. E-mails must include "Extended Application" and the team reference number in the subject line.

(2) Mailed/hand-carried directly to DARPA. Application materials must be addressed to:

DARPA/I2O
Attn: Cyber Grand Challenge
675 North Randolph Street
Arlington, VA 22203-2114

Application materials received after the deadline specified herein will be disposed of in a secure manner. Application materials will not be returned. Incomplete applications will not be accepted. DARPA may disqualify any team which does not meet the eligibility requirements specified herein.

3 Cyber Grand Challenge Events

3.1 Cyber Grand Challenge Qualification Event (CQE)

Finalists for the CFE will be determined at the CQE. The CQE is tentatively scheduled for June 3, 2015. During the CQE, all Proposal Track and Open Track competitors will receive an identical corpus of Challenge Binaries (CBs): insecure software which must be analyzed and secured. The goal of the CQE is to use an autonomous system to locate and mitigate flaws in the CBs and return a corpus of CB data to DARPA for scoring.

3.1.1 Preparing for CQE

Competitors will have the opportunity to participate in two preliminary Scored Events that will be similar in format to the CQE. Participation in these Scored Events is optional and success in these events will not be evaluated as part of CGC scoring. Each Scored Event is an opportunity for competitors to gain an understanding of the format, procedure, and scoring mechanism to be used during the CQE. These events are tentatively scheduled for December 2, 2014 and April 6, 2015.

3.1.2 CQE Scoring

Proposal Track and Open Track competitors will receive a score based on their ability to locate and mitigate flaws in CB software while minimizing damage to the function of each CB. The CQE will involve securing a corpus of over 100 CBs. For each CB, a CRS will demonstrate the location of existing flaws by formulating inputs that activate a software

flaw, crash or fault. To demonstrate the mitigation of flaws, each CRS will provide a secured version of each CB. Scoring will reflect performance in CQE AoE 1 - 4 as indicated in Table 1. A CRS must mitigate a flaw in at least one CB while retaining some CB functionality in order to receive a score greater than zero.

3.1.3 Advancement to CFE

Using a scoring methodology derived from AoE 1 - 4, DARPA will score and rank teams from the Proposal Track and Open Tracks. Based on this scoring, DARPA will invite some teams to the CFE as finalists. Finalists invited by DARPA will:

- Have submitted a CQE Technical Paper accepted by DARPA,
- Achieve a top ranking, non-zero CQE score, and
- Have successfully demonstrated their system to DARPA during a site visit.

3.1.3.1 CQE Technical Paper

To receive an invitation to the CFE, a team must submit an acceptable CQE technical paper to DARPA describing their CRS. CQE technical papers will be evaluated and approved according to the CGC Technical Paper Guidelines to be posted on the CGC website: www.darpa.mil/cybergrandchallenge. DARPA will review each technical paper and communicate acceptance of papers to each team leader. CQE Technical Papers are due March 5, 2015.

3.1.3.2 Site Visit

After CQE performance, teams must demonstrate the function of their system during a team site visit. DARPA will travel to an acceptable location (within the United States) identified by each eligible team. DARPA will release the Site Visit Procedures on or before June 3, 2014. Each team leader and CRS must be present at the site visit. DARPA will bring a corpus of CB software to the demonstration for analysis by the CRS. DARPA will assess the CRS using the CQE AoE listed in Table 1. During the site visit, teams should be prepared to demonstrate the CRS to the satisfaction of the DARPA team.

3.1.4 Finalists

Proposal Track teams invited to the CFE as finalists will continue to be funded by DARPA through their period of performance, in accordance with the terms of their awards. (See DARPA-BAA-14-05 for details). Proposal Track teams are not eligible to win prizes at the CQE stage.

Open Track teams invited to the CFE as finalists will receive a cash prize and retain eligibility to compete in the CFE. The anticipated amount of CQE prizes is $750,000 per invited team.

3.2 Cyber Grand Challenge Final Event (CFE)

The CGC Champion will be determined at the CFE, tentatively scheduled for July 17, 2016. The CFE will consist of a real time, all-computer tournament scored over all Areas of Excellence from Table 1.

3.2.1 CFE Trials

To demonstrate readiness for the CFE, each finalist CRS will be required to pass a series of three Trials. These Trials (described below) are intended to demonstrate the field-worthiness of each finalist CRS and present an opportunity for competitors to debug and refine interactions with the Competition Framework prior to CFE competition. Over a three-week period, DARPA will provide each finalist with access to the Competition Framework to allow a demonstration match against a simulated opponent.

> Trial 1 demonstrates ability in Area of Excellence 4. To pass this trial, each CRS will receive a Challenge Binary from the Competition Framework and field it on a networked host without disrupting its intended function.
>
> Trial 2 demonstrates ability in Areas of Excellence 2 and 5. To pass this trial, competitor systems receive a Challenge Binary from the Competition Framework and field it on a networked host while preventing attempts by a simulated competitor to activate any flaws in the CB.
>
> Trial 3 demonstrates ability in Area of Excellence 3. To pass this trial, competitor systems receive a Challenge Binary from the Competition Framework, identify its presence and remotely activate a flaw in the CB as it exists on a networked host operated by a simulated opponent.

Note that the Trials do not address Area of Excellence 1. Challenge Binaries for the Trials will be provided to competitors beforehand, and competitors are welcome to field signatures, patches, and vulnerability scans which have been hand crafted prior to the Trials.

DARPA will provide notification to each finalist as each Trial is completed. Upon completion of all three Trials, DARPA will issue a certification to each successful finalist. DARPA may, at its sole discretion, disqualify any finalist team which does not complete the Trials within the three week period.

The CFE Trial series is the only CGC event in which automated program analysis is not required. See Section 4 for further information on automation requirements.

3.2.2 CFE Format

During the CFE, each finalist will field a CRS. Each CRS will interface with the CGC Competition Framework via a networked interface to be specified by DARPA in the CGC Competition Framework API. This interface will provide each CRS with access to CBs as well as a networked host on which each CB must be fielded. During the CFE, each CRS will be responsible for maintaining and securing CB software provided by the Competition Framework; each CRS will be responsible for deploying this software on a networked host. Each CRS will have the ability to administer its own networked host, as well as connect to networked hosts operated by other finalists. Each CRS will work to challenge other finalists by emitting Proofs of Vulnerability (Area of Excellence 3) directed at the networked hosts operated by competitors. In turn, each CRS will work to repel such proofs from its own system, utilizing AoE 1, 2, and 5. The Competition Framework will provide extensive monitoring of the health of all CB software in operation, noting when competitors fail to keep software running and undamaged (Area of Excellence 4).

The CFE is designed to pose realistic defense challenges. For this reason, the CRS confronts the CFE network from the vantage point of a real world network defender. Each CRS <u>will</u> have the ability to deploy CBs to a networked host as well as monitor and modify network traffic to a networked host. Teams <u>will not</u> have the ability to alter the operating system or hardware of the networked host, or harness the execution of CBs as they operate *in situ.* For this reason, approaches that require a defended host to use custom hardware, custom operating system modifications, or harnessed software execution will be unable to interface with the Competition Framework.

A CRS observing network traffic during the CFE will be prevented from identifying the originating system of each connection via technical means imposed by the Competition Framework. Due to this limitation, decisions about network traffic made by a CRS must be made based on the contents of the network traffic rather than network addressing information.

3.2.3 CFE Scoring

The scoring methodology for the CFE will be announced by DARPA following the selection of CFE finalists. The scoring methodology will reflect successful cyber reasoning during a live exercise utilizing the CFE AoE identified in Table 1. This score will include the following considerations:

- A successful CRS will mitigate all vulnerabilities in the CB software running on its networked host, using whatever combination of networked defense or security patching is appropriate, without degrading the availability or correct function of each CB.

- A successful CRS will challenge the CB software maintained by competitors on their networked hosts; this will be accomplished by emitting Proofs of Vulnerability to the CB software.

- An unsuccessful CRS will fail to maintain the function of CB software on its networked host.

- An unsuccessful CRS will repeatedly allow Proofs of Vulnerability from other competitors to activate flaws in CB software.

At the conclusion of the event, DARPA will consult with event monitors to confirm the scoring results and the integrity of the competition.

3.2.4 CFE Technical Paper

All CFE participants must submit a CFE Technical Paper to DARPA describing their CRS in its final competition state, as well as lessons learned during CFE. CFE technical papers will be evaluated and approved according to the CGC Technical Paper Guidelines. DARPA will review each technical paper and communicate acceptance of papers to each performer. CFE Technical Papers are due within three weeks of the conclusion of the CFE.

3.2.5 CFE Prizes

Based on finalized scoring, DARPA will determine 1st, 2nd, and 3rd place winners to receive prizes. Following receipt and acceptance of final CFE Technical Papers from each winning team, DARPA will publicly announce the 1st, 2nd and 3rd place winners.

DARPA anticipates prizes in the following amounts:

- 1st place: $2,000,000
- 2nd place: $1,000,000
- 3rd place: $750,000

Both Proposal Track and Open Track teams are eligible to receive prizes following the CFE.

4 Full Automation Requirement

Both the CQE and the CFE require a fully automated solution – no human assistance is permitted during either event in any cyber reasoning processes, including reverse engineering and patch formulation. Human assistance or other violation of these rules during CGC events will result in team disqualification and further actions as appropriate under Federal law and regulation. DARPA will preserve the integrity of competition within the CGC with safeguards to be developed during the program. These safeguards

will not be shared as sharing may cause the methods to be ineffective. For this reason, all safeguard inspection schedules, methods, and capabilities will not be disclosed to any Challenge participant for any reason. Any information regarding human interference in cyber reasoning processes during any CGC event should be sent to CyberGrandChallenge@darpa.mil.

5 Intellectual Property

DARPA claims no rights to software developed by Open Track competitors as a result of participation in the CGC. DARPA does not intend to disclose the CQE and CFE Technical Papers outside the Government, with the following exception: CGC Technical Papers may be handled by DARPA support contractors for administrative purposes and/or to assist with technical evaluation. All DARPA support contractors performing this role are bound by nondisclosure agreements. DARPA does not intend to disclose CGC Technical Papers to contractors to duplicate, commercialize, or for reprocurement or reverse engineering purposes.

Proposal Track competitors should refer to DARPA-BAA-14-05 for specific information on intellectual property (IP) licensing rights related to their participation.

6 Additional Information

The development of revolutionary technologies is a key objective of the CGC. Teams are invited to communicate directly with DARPA regarding any rule that restricts their ability to demonstrate technical achievement and innovative solutions. Questions regarding rules should be sent to CyberGrandChallenge@darpa.mil.

DARPA may modify the rules at any time and for any reason, including the accommodation of a promising technical approach that would have been excluded by the rules.

DARPA unilaterally reserves the right to cancel or modify the CQE and CFE at its sole discretion. Considerations may include availability of funds and technical viability.

Participation in the CQE and CFE will be governed by Event Participation Agreements to be released by DARPA [4]. These Agreements will define the boundaries of competition within each event as well as assign IP rights to data transmitted during each event to DARPA. Acceptance of the Event Participation Agreements is mandatory for event participation. All data generated by each CRS during the CFE, to include network traffic, modified CBs, network host status, and other output data will be logged by the Competition Framework. These logs will be released into the public domain.

[4] The Event Participation Agreements will be posted on the CGC website at www.darpa.mil/cybergrandchallenge.

The CGC prize is authorized under 15 U.S.C. § 3719. The CGC program will incentivize innovation using multiple cash prizes.[5]

In accordance with 15 U.S.C. § 3719, to be eligible to win a prize in this Challenge, an individual must have applied to participate in the Challenge in accordance with the instructions outlined herein. The entrant (described in section 2.1) shall be the prize recipient. The prize recipient shall be a citizen, a permanent resident of the United States, or a US Entity. Tax treatment of prizes will be handled in accordance with U.S. Internal Revenue Service guidelines.

Application information collected by DARPA will be used solely for the purpose of administering the CGC. Use of application information is governed by the Privacy Policy posted on the Cyber Grand Challenge website.

Teams may be listed on the CGC website to enable the event to be tracked by interested members of the public. The name and photographs of the winning teams may be posted on the DARPA website and released to the media.

DARPA reserves the right to disqualify a participant whose actions are deemed to violate the spirit of the competition for any reason, including but not limited to, the violation of relevant laws or regulations in the course of participation in the CGC.

By applying to and/or participating in the CGC, applicants and participants agree to follow these rules. Applicants and participants must agree to assume any and all risks and waive claims against the Federal Government and its related entities, except in the case of willful misconduct, for any injury, death, damage, or loss of property, revenue, or profits, whether direct, indirect, or consequential, arising from participation in the competition, whether the injury death, damage, or loss arises through negligence or otherwise.

DARPA does not authorize or consent to CGC participants infringing on any U.S. patent or copyright while participating in the CGC. No illegal activities may be undertaken for the purpose of participation in the Cyber Grand Challenge.

The appearance and reference to any person, name, place, film, artwork or any other images that are used in connection with the CGC does not constitute or imply endorsement by the U.S. Department of Defense or by DARPA.

Questions regarding the rules, privacy policy, or other aspects of the CGC may be directed to CyberGrandChallenge@darpa.mil.

[5] Trophies will be substituted for cash prizes in the absence of sufficient funds.

7 Scope and Precedence

The rules outlined herein apply to all applicants and participants in the CGC. However, nothing in these rules, to include this document and any subsequent CGC rules documents, may be interpreted as modifying the statement of work or authorizing work outside the terms and conditions of any existing agreements or contracts with DARPA.

DARPA will release additional documents with rules updates, procedures, and other information for teams. These additional documents carry the full authority of the rules in this document.

Additional documents to be released include the following, at a minimum:

CGC Documents:

- CGC Master Schedule
- CGC Technical Paper Guidelines
- CGC Site Visit Procedures
- CGC Extended Application

CGC Qualification Event (CQE) Documents:

- CQE Procedures
- CQE Scoring Guide

CGC Final Event (CFE) Documents:

- Competition Framework API Document
- CFE Procedures
- CFE Scoring Guide

All documents including this Rules document will be posted and updated on the CGC website, www.darpa.mil/cybergrandchallenge. All CGC documents including these Rules should be considered living documents, subject to update and clarification throughout the CGC program.